Blockchain consensus: From proof-of work to proof-of-stake

Jonathan Healy
jonathan.d.healy@gmail.com
January 2020

1. Introduction

With the introduction of Bitcoin in 2008 via the Bitcoin white paper [1] written by an author cloaked in anonymity – Satoshi Nakamoto - the notion of the blockchain was introduced to the world. The consensus model for Bitcoin is called proof-of-work. Nodes in the network seeking to acquire rewards, associated with adding a block of transactions to the inter-connected chain of blocks that stretch right back to the very genesis block itself, compete to compute cryptographic puzzles. After a valid block of transactions is assembled and a hash containing enough leading zeroes is found for that block, the block is examined by other nodes in the network.

Process is important here because the system relies on it to provide security and ensure that the double-spending problem is solved. Solving this problem guarantees that the same unit of currency will not be spent twice. Prior to the introduction of Bitcoin this was something that was unsolved. Over the years confidence in Bitcoin has grown and today the network has a market cap of over $157 billion dollars measured in US currency invested in it. There are two main criticisms of Bitcoin however.

One criticism of Bitcoin is that the network is slow and the other concerns the vast amounts of energy via electricity that is presently being used to secure the Bitcoin blockchain. Both of these things can be addressed by improving Bitcoin's consensus model. The most popular idea with respect to replacing proof-of-work is easily proof-of-stake. In this system nodes are generally chosen to validate a block of transactions and receive the corresponding reward with the odds of doing so being based on the number of tokens that are held in a node's account [2,3,4,5].

2. Proof-of-Stake

3. Pure Proof-of-Stake

Algorand is a blockchain group headed by former Turing award winner Silvio Micali that uses an alternate version of proof-of-stake called pure proof-of-stake (PPoS) alongside their novel implementation of pseudo-random functions built on Byzantine consensus [2].

References

1. Nakamoto, Satoshi. *Bitcoin: A peer-to-peer electronic cash system*. 2008.
2. Gilad, Yossi, et al. "Algorand: Scaling byzantine agreements for cryptocurrencies." *Proceedings of the 26th Symposium on Operating Systems Principles*. 2017.
3.